Eur. Phys. J. D (2020) 74: 33
https://doi.org/10.1140/epjd/e2019-100385-y

THE EUROPEAN PHYSICAL JOURNAL D

Regular Article

Teleportation-based quantum secure communication using quantum channel compression

Georgi Bebrov[a] and Rozalina Dimova

Telecommunications Department, Technical University of Varna, Varna 9010, Bulgaria

Received 8 August 2019 / Received in final form 5 November 2019
Published online 20 February 2020
© EDP Sciences / Società Italiana di Fisica / Springer-Verlag GmbH Germany, part of Springer Nature, 2020

Abstract. The paper proposes a scheme for quantum secure communication of key strings, which is based on maximally entangled pairs (EPR pairs), teleportation, and quantum channel compression (QCC). Having ensured the security of their quantum channel by means of a standard eavesdropping check communication (called here "QCC eavesdropping check communication"), Alice and Bob begin the message translation phase. The latter consists of three steps: (i) encoding (QCC encoding) data into single-qubit systems according to the message (key sequence) intended to be transferred from Alice to Bob, (ii) teleporting the encoded single-qubit systems over the established secure quantum channel, and (iii) extracting (QCC decoding) data from the received via teleportation single-qubit systems. The novel teleportation-based quantum secure communication is characterized with efficiency higher than the efficiency of any other scheme of the same type.

1 Introduction

In the zenith of the information age, the requirement for confidential communication becomes more and more stringent. The only communication methods that can ensure unconditional security are those of quantum cryptography. The quantum cryptographic methods (protocols) can principally fall into one of the two groups: quantum key distribution (QKD) and quantum secure communication (QSC). The QKD [1–3], which marks the beginning of the field of quantum cryptography, describes approaches in which two or more parties establish a secure cryptographic key by using quantum phenomena (entanglement, uncertainty principle [25]). On the other hand, the QSC [4–19] describes approaches in which two or more parties communicate in a secure manner by using quantum phenomena. In this type of secure communication, the parties could exchange cryptographic keys more efficiently than QKD. It is known that one can encounter two types of QSC: quantum secure direct communication (QSDC) [4–8] and deterministic secure quantum communication (DSQC) [9–19]. In the QSDC, the message (key) is transferred only by using a quantum channel. On the contrary, in the DSQC the message is transferred by both quantum and classical channels – to be more precise, an auxiliary classical information is required for reading out a message encoded in quantum systems.

A profound way to perform a DSQC is by using the process of quantum teleportation [9–11]. The first secure communication protocol of this type is proposed by Yan and Zhang [9]. Other protocols based on the teleportation process are given in [10–14]. Using teleportation has several advantages, as pointed out in [9,10]: a protocol based on teleportation is more secure even in noisy channel [16], is suitable for quantum error correction [15], and offers a communication without transmitting the qubit, which carries the secret message, over an insecure channel [9].

In this paper, a teleportation-based DSQC protocol, which uses quantum channel compression [20], is proposed for the needs of cryptographic keys distribution. In this novel model, by using the quantum channel compression (QCC) the sender encodes two bits of information into each teleported qubit. The recipient extracts the information from the teleported qubits by measuring them and using an appropriate decoding procedure. In order for the decoding to be properly performed, an additional information, embedded in the eavesdropping check (detection) process, is employed.

The present article is organized as follows. In Section 2, the process of quantum channel compression is presented. In Section 3, the process of teleportation, used in the newly proposed scheme, is described. In Section 4, the novel teleportation-based DSQC protocol is introduced. In Section 5, efficiency and security analyses for the proposed protocol are set out. In Section 6, we put forward conclusions.

2 QCC procedure incorporated into the novel scheme

The QCC process is conformed to the features of quantum secure communication schemes (protocols). It consists of

[a] e-mail: g.bebrov@tu-varna.bg

Table 1. Encoding table for all the two-bit symbols X_i of the message, except X_0 (Y_i – encoded two-bit symbols).

Y_{i-1}/X_0	X_i	Y_i	Y_{i-1}/X_0	X_i	Y_i
00	00	01	01	00	00
00	01	10	01	01	11
00	10	11	01	10	10
00	11	00	01	11	01
10	00	10	11	00	11
10	01	01	11	01	00
10	10	00	11	10	01
10	11	11	11	11	10

Table 2. Encoding table for the first two-bit symbol of the message, X_0.

$\mathrm{XOR}(Y_j^0)$	$\mathrm{XOR}(Y_j^1)$	X_0	Y_0	X_0	Y_0
0	0	00	00	01	11
0	1	00	01	01	00
1	0	00	10	01	01
1	1	00	11	01	10
0	0	10	10	11	01
0	1	10	11	11	10
1	0	10	00	11	11
1	1	10	01	11	00

three steps: encoding, eavesdropping check communication, and decoding. The appropriate QCC steps for a novel teleportation-based quantum secure communication scheme (Sect. 4) are respectively considered in the following subsections.

2.1 QCC encoding/decoding

The encoding is characterized by the function

$$f : X_i \in \{0,1\}^2 \rightarrow Y_i \in \{0,1\}^2 | Y_{i-1}(\text{or } X_0), X_i.$$

It can be explained as follows.

Each two-bit symbol X_i of a message string X is encoded into a two-bit symbol Y_i of an encoded string Y with regard to the values of the symbols Y_{i-1} (or X_0 when X_1 is encoded) and X_i, as shown in Table 1. Exception is made for the first symbol X_0, which is encoded into Y_0 with regard to $\mathrm{XOR}(Y_j^0)$ and $\mathrm{XOR}(Y_j^1)$, as shown in Table 2. The entities $\mathrm{XOR}(Y_j^0)$ and $\mathrm{XOR}(Y_j^1)$ are obtained by

$$\mathrm{XOR}(Y_j^0) = \bigoplus_{j=1}^{N-1} Y_j^0, \quad (1)$$

$$\mathrm{XOR}(Y_j^1) = \bigoplus_{j=1}^{N-1} Y_j^1. \quad (2)$$

The symbol Y_j^1 indicates the least significant bit (LSB) of Y_j, whereas Y_j^0 indicates the most significant bit (MSB) of Y_j. The index j goes from 1 to $N-1$, unlike the index i which goes from 0 to $N-1$.

In the quantum secure communication protocols, the classical message is transferred by quantum systems. In our case, we transfer the message (the encoded symbols Y_is) by qubits: 00 and 11 are respectively transferred by $|+\rangle$ and $|-\rangle$ (diagonal basis), whereas 01 and 10 are respectively transferred by $|R\rangle$ ($|y+\rangle$) and $|L\rangle$ ($|y-\rangle$) (circular basis). This means that we perform a mapping q: $\{0,1\}^2 \rightarrow \{|+\rangle, |-\rangle, |R\rangle, |L\rangle\}$, which converts the string Y_i into the string of qubits Q_i.

Along with the conversions $X_i \rightarrow Y_i$ and $Y_i \rightarrow Q_i$, an additional string b_i is formed in the encoding process. This is a string that facilitates the decoding procedure. The elements of the string b_i are obtained as follows:

$$b_i = 0 \text{ if } Y_i = 00 \text{ or } 11, \text{ and } b_i = 1 \text{ if } Y_i = 01 \text{ or } 10.$$

That is, each b_i indicates which basis has to be used for measuring each Q_i ($b_i = 0$ – diagonal basis, $b_i = 1$ – circular basis). The string b_i is used by the recipient for performing proper decoding.

The decoding is performed in a reverse order: (1) receiving the qubits Q_i, (2) measuring Q_i by taking into account b_i (obtaining Y_i), and (3) decoding Y_i in terms of Tables 1 and 2 (extracting X_i).

For the sake of clarity, we explain the encoding by the way of the following example. Suppose we have the binary message (key string)

$$1001110010010110.$$

First, we divide the message into two-bit symbols X_i:

$$10|01|11|00|10|01|01|10.$$

Secondly, according to Tables 1 and 2, we encode the two-bit symbols as follows (the first symbol is the last encoded; we first start off with the second symbol X_1)
$X_1 = 01$, $X_0 = 10$ $\Rightarrow Y_1 = 01$; $X_2 = 11, Y_1 = 01$ $\Rightarrow Y_2 = 01$;
$X_3 = 00$, $Y_2 = 01$ $\Rightarrow Y_3 = 00$; $X_4 = 10$, $Y_3 = 00$ $\Rightarrow Y_4 = 11$;
$X_5 = 01$, $Y_4 = 11$ $\Rightarrow Y_5 = 00$; $X_6 = 01$, $Y_5 = 00$ $\Rightarrow Y_6 = 10$;
$X_7 = 10$, $Y_6 = 10$ $\Rightarrow Y_7 = 00$ (see Tab. 1).
And at last,
$X_0 = 10$, $\mathrm{XOR}(Y_j^0) = 0 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$, and $\mathrm{XOR}(Y_j^1) = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 1 \Rightarrow Y_0 = 11$ (see Tab. 2).
So, we obtain the encoded message Y

$$11|01|01|00|11|00|10|00.$$

We transfer the encoded message by the following qubit string

$$|-\rangle |R\rangle |R\rangle |+\rangle |-\rangle |+\rangle |L\rangle |+\rangle .$$

We also form the "basis" string b_i, which indicates the bases of the qubits in the qubit string:

$$01100010.$$

Note: In the teleportation-based protocol to be proposed later on, the b_is are transferred alongside the results of the Bell measurements performed for achieving teleportation.

2.2 QCC eavesdropping check communication

In the scheme we propose herein, we employ a standard eavesdropping check communication. It consists of three messages: ACK, DCY, and BAS. Assume that two parties, Alice and Bob, in a quantum secure communication share EPR pairs. That is, one party prepares the EPR pairs and sends to the other party a group (quanta group) consisting of one of the entanglings[1] of these EPR pairs. In this context, the message ACK is used to inform the sender whether or not the quantum systems are received by the recipient.

The message DCY is used by one party to inform the other one about the positions of the decoy systems that are used for checking the presence of an eavesdropper [4–7,9–11,15–17,19]. This message is a string of binary digits, zeros and ones: "0" indicates a data system, whereas "1" indicates a decoy system. For instance, suppose that two parties share ten EPR pairs and the following DCY message is exchanged between them:

$$0100110101.$$

This implies that the EPR pairs in positions 2, 5, 6, 8, and 10 are decoys.

The message BAS is used to give information about: (1) the bases that are used for measuring the decoy systems; (2) the results of those measurements.

3 Teleportation procedure

Suppose Alice sends a two-bit symbol to Bob via a teleportation process. Suppose further that Alice and Bob share a quantum channel (Bell pair)

$$\left|\Phi^{+}\right\rangle_{AB} = \frac{1}{\sqrt{2}}(\left|00\right\rangle_{AB} + \left|11\right\rangle_{AB}), \tag{3}$$

which is used to teleport a qubit being in the state

$$\left|\Psi_T\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle_T + a\left|1\right\rangle_T), \tag{4}$$

where $a \in \{1, -1, i, -i\}$: $a = 1$, $a = -1$, $a = i$, and $a = -i$ correspond to $|+\rangle$, $|-\rangle$, $|R\rangle$, and $|L\rangle$, respectively. As obtained in [9], the overall state of the system ABT is

$$\begin{aligned}\left|\Phi^{+}\right\rangle_{AB}\left|\Psi\right\rangle_T &= \frac{1}{2}(\left|00\right\rangle_{AB} + \left|11\right\rangle_{AB})(\left|0\right\rangle_T + a\left|1\right\rangle_T)\\ &= \frac{1}{2\sqrt{2}}[(\left|0\right\rangle_B + a\left|1\right\rangle_B)\left|\Phi^{+}\right\rangle_{AT}\\ &\quad + (\left|0\right\rangle_B - a\left|1\right\rangle_B)\left|\Phi^{-}\right\rangle_{AT}\\ &\quad + (a\left|0\right\rangle_B + \left|1\right\rangle_B)\left|\Psi^{+}\right\rangle_{AT}\\ &\quad + (a\left|0\right\rangle_B - \left|1\right\rangle_B)\left|\Psi^{-}\right\rangle_{AT}].\end{aligned} \tag{5}$$

[1] Entangling – a quantum particle, which takes part in an entangled system.

After a Bell measurement performed by Alice, Bob's particle will be in either of the following possible states [9]

$$\frac{1}{\sqrt{2}}(\left|0\right\rangle_B + a\left|1\right\rangle_B) = U_{00}\left|\Psi\right\rangle_T, \tag{6}$$

$$\frac{1}{\sqrt{2}}(\left|0\right\rangle_B - a\left|1\right\rangle_B) = U_{01}\left|\Psi\right\rangle_T, \tag{7}$$

$$\frac{1}{\sqrt{2}}(a\left|0\right\rangle_B + \left|1\right\rangle_B) = U_{10}\left|\Psi\right\rangle_T, \tag{8}$$

$$\frac{1}{\sqrt{2}}(a\left|0\right\rangle_B - \left|1\right\rangle_B) = U_{11}\left|\Psi\right\rangle_T, \tag{9}$$

where

$$U_{00} = \begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}, U_{01} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, U_{10} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, U_{11} = \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}. \tag{10}$$

That is, in order to obtain the original state, Bob needs to perform one of the U_{ij} operations on the received state. Because the $U_{ij}s$ depend on the result of the Bell measurement carried out by Alice, she sends to Bob a two-bit message that indicates which U_{ij} should be performed by Bob.

In our scheme, in addition to the two-bit message Alice should send another single-bit message indicating the basis in which Bob has to measure the received quantum state. The reason for this is that the states $|+\rangle$, $|-\rangle$ and $|R\rangle$, $|L\rangle$ are respectively from two different mutually unbiased bases – diagonal and circular. So, in order for Bob to correctly extract the original message from the teleported qubit, he should also know the basis in which that qubit should be measured. In the DSQC protocol proposed in the next section, the basis information is carried by the physical bits of the string b, which was described in Section 2.1.

4 Novel teleportation-based quantum secure communication protocol

The proposed protocol is based on the teleportation-based quantum secure communication protocol of [9], except that a QCC is used. That is why, some of the protocol steps presented below coincide with those of the mentioned scheme. The protocol steps of the novel secure communication scheme are:

Step 1. Alice encodes a N-bit message (N is an even integer number) she wishes to send to Bob. The approach presented in Section 2.1 is used for that purpose.

Step 2. Bob prepares $N/2$ EPR pairs, all in the state $|\Phi^{+}\rangle$. Then, he sends their second entanglings to Alice (EPR pairs sharing is performed).

Step 3. In this step the QCC eavesdropping check communication from Section 2.2 is performed. Alice sends to Bob an ACK message, i.e., confirms the reception of the particles of step 2. If the ACK message is positive, Alice sends DCY message to Bob,

i.e., tells Bob which $N/4$ pairs play the role of decoy systems. Alice measures each of her decoys in a randomly chosen basis (either rectilinear or diagonal polarization basis). Then, Alice sends BAS message to Bob, i.e., informs Bob about the bases she chose in the decoy measurements and about the results of these measurements.

Step 4. Based on the DCY and BAS messages from Alice, Bob measures his parts of the decoy EPR pairs and evaluates (Error rate evaluation is performed) the correlation between his results and those of Alice. If there is a discrepancy (in %), an error rate, exceeding a predetermined threshold value, Alice and Bob shut down the current session and start over the protocol they go back to step 2. Otherwise, they proceed forward to the next step.

Step 5. According to the encoded message (string Y) that Alice wishes to send to Bob, she prepares $N/2$ single-qubit systems (teleportlings[2]), as each system is set in either $|+\rangle$ (for encoded symbol $Y_i = 00$), or $|-\rangle$ (for $Y_i = 11$), or $|L\rangle$ (for $Y_i = 01$), or $|R\rangle$ (for $Y_i = 10$). Then, Alice teleports these single-qubit systems using the approach presented in Section 3 and used in [9]: (i) Alice performs a Bell measurement on the teleportlings and the EPR entanglings of her possession; (ii) Alice sends to Bob auxiliary classical data (2 bits for each teleportling) in order for him to be able to properly receive the teleported states. Along with the auxiliary classical bits of (ii), Alice announces additional bits, b_i (see Sect. 2.1), with the help of which the encoded message, string Y, is properly transferred to Bob.

Step 6. Having the DCY message and string Y (the encoded message), Bob performs the QCC decoding mentioned in Section 2.1 in order to retrieve the original key string.

Step 7. Because errors always occur in the quantum channel, error-correction algorithm is performed on the received key string [22]. Also, in order to prevent data leaking to the eavesdropper, a privacy amplification algorithm is carried out [21].

A sequence diagram depicting the proposed protocol is shown in Figure 1.

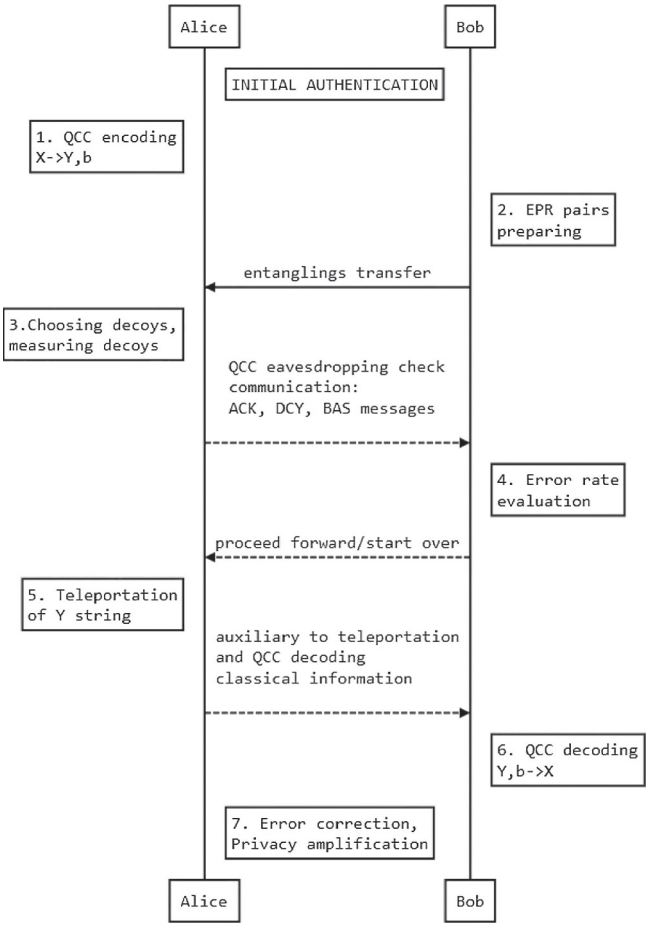

Fig. 1. A sequence diagram describing the communication between Alice and Bob (sender and recipient) in the proposed teleportation-based quantum secure communication protocol (normal line – quantum channel, dashed line – classical channel).

5 Efficiency and security analyses

5.1 Efficiency analysis

In this section, we calculate the efficiency of the proposed protocol as well as compare it to other existing schemes of teleportation-based type. The proposed protocol is a set of identical teleportation procedures, that is, the overall efficiency of the protocol can be evaluated as follows

$$E' = \text{avg}(E) \text{ over all the teleportation procedures,} \quad (11)$$

where E is the efficiency of a single teleportation procedure. Because the procedures are identical, the above expression transforms into the equality $E = E$. We decide the efficiency of a single teleportation procedure to be evaluated by [23]

$$E = \frac{b_s}{q_t + b_t}, \quad (12)$$

where b_s is the number of physical bits transferred in a procedure of the protocol, q_t and b_t are the number of qubits and auxiliary bits, respectively, used for transferring the $b_s s$ in a secure manner. In this expression, the qubits q_t incorporate the number of both data and decoy qubit systems: $q_t = q_d + q_D$, where q_d accounts for the number of decoys (EPR decoy quantum channels) and q_D for the number of data systems (EPR quantum channels used to teleport data qubits). Note that the bits of the b string (b_i) should be regarded as auxiliary bits, since they are used for retrieving the data from the quantum systems – in the case of the proposed protocol, for retrieving data from each teleported qubit we need an additional auxiliary bit b_i (see Sect. 2.1), in comparison to the standard pro-

[2] Teleportling – a quantum system, which undergoes a teleportation procedure.

Table 3. Efficiency comparison of teleportation-based direct secure quantum communication protocols (PP – the protocol proposed in this paper).

Protocol	Efficiency	Quantum channel
YZ04 [9]	0.1667	Bell pair
JSM17 [10]	0.25	GHZ-like state
JSM17 [10]	0.2143	Five-qubit Brown state
XGC09 [11]	0.1875	Six-particle state
PP	0.286	Bell pair

tocol [9]. Then, according to the above equation and the equality $E' = E$ the efficiency of the proposed protocol is

$$E = \frac{b_s}{(q_d + q_D) + b_t} = \frac{2}{(2+2)+3} = \frac{2}{7} = 0.286. \quad (13)$$

That is, equation (13) shows that each two-bit data symbol X_i is transferred by using a single teleportation procedure, which requires two-qubit data channel (Bell pair), two-qubit decoy system (Bell pair), and three-bit auxiliary classical channel.

Next, we compare the proposed protocol in terms of efficiency to existing protocols of the same type [9–11]. The values of the efficiencies of these protocols are taken from [10] (see Tab. 3 in this reference). The latter as well as the value calculated in equation (13) are tabulated in Table 3. As can be readily seen, the herein proposed protocol exceeds the efficiencies of the other protocols. However, note that in order for the efficiency of 0.286 to be obtained in the proposed scheme, the practicality is reduced more complex encoding and decoding processes (devices, respectively) are utilized.

5.2 Security analysis

In general, the security analysis of a quantum secure communication scheme is performed only in terms of the quantum channel. However, in this paper we perform also a security analysis in terms of the classical public channel. Because the classical channel plays an important role in the proposed protocol, as important as the quantum channel (unlike the standard protocols [9–11]), we present in detail its security analysis. On the other hand, a security analysis in terms of the quantum channel is not given. The reason for this is the fact that the proposed protocol is identical to the scheme [9] with regard to the quantum communication, i.e., they share the same security analysis.

In order for the scheme to be secure, (1) the eavesdropper should not gain any information about the message X_i if she knows the basis string b_i, (2) the value of X_0 should be completely concealed (the eavesdropper should be uncertain about it when knowing b_i as well as knowing Y_0).

Before proving that these requirements (1) and (2) are met by the proposed protocol, we would like to set out essential for the proofs entities. The entities of concern are $H(X_i)$, $H(Y_i)$ – the entropies of the variables $X_i s$ and $Y_i s$, which are used for evaluating the uncertainty about the values of these variables.

Because by the proposed protocol we transfer key strings (random strings), each key symbol X_i is assumed to be a random variable – $X_i \in \{0,1\}^2$ with uniform distribution ($X_i \sim$ unif). Therefore, the entropy $H(X_i) = 2$ [24].

The entity $H(Y_i)$ is more difficult to be calculated, because we first need to find out the probability distributions of the $Y_i s$. Let y and x indicate the possible outcomes (values) of the variables Y_i and X_i – i.e., y, $x \in$ 00,01,10,11. In the following, we analyze each Y_i independently (*Note*: We take for granted that the variable Y_0 is a uniformly random variable – we verify that later on in this section). The probability distribution of Y_1 is uniform ($\Pr(Y_1 = y) = 0.25$), since its value y depends entirely on the uniformly random variable X_0. The probability distribution of Y_2 is also assumed to be uniform ($\Pr(Y_2 = y) = 0.25$), because its value depends on Y_1 and X_1 – a variable, which depends only on uniformly random variables, is also a uniformly random variable. Since all the Y_i are obtained in one and the same way, it is straightforward to verify that the statement about Y_2 holds for all the other $Y_i s$, too. Therefore, we get $H(Y_i) = 2$ for any Y_i, i.e., the whole string Y has such an entropy – $H(Y) = 2$.

We are now in a position to prove that the requirements (1) and (2) are met by the proposed protocol.

Proof that the requirement (1) is met: This requirement can be symbolically stated as $I(X; b) = 0$ bit. For the sake of simplicity and brevity, in the following lines we show $I(X_i; b) = 0$ – knowing the string b, the eavesdropper cannot learn any information about a given (any) message symbol X_i.

In order to learn a given (any except X_0 and X_1) X_i, one should know its corresponding (with regard to the encoding) pair of encoded symbols $Y_{i-1}Y_i$ (*Note*: X_1 depends on the pair (X_0,Y_1), whereas X_0 depends on the pair ($\mathrm{XOR}(Y_j^0)$,$\mathrm{XOR}(Y_j^1)$)). Thus, we should prove that knowing all the $b_i s$, the eavesdropper cannot deduce with certainty the values of $Y_{i-1}Y_i$. One thing that gives information about the Y string is the b string:

Knowing b_i implies that the eavesdropper knows partially the string $Y_i \rightarrow H(Y_i|b_i) = 1$, instead of the maximum value 2. This comes from the fact that knowing the basis in which a qubit has to be measured, the eavesdropper gains one half of the information transferred by the qubit. So, the eavesdropper gains 1 bit of information (out of 2) about (for) each Y_i. We use the mutual information to evaluate this information leakage [25]:

$$I(Y_i; b_i) = H(Y_i) - H(Y_i|b_i) = 2 - 1 = 1 \text{ bit}. \quad (14)$$

However, to learn a given X_i, the eavesdropper needs to know the pair $Y_{i-1}Y_i$ – this comes from the encoding procedure. Then, how much information does the pair $b_{i-1}b_i$ give about the pair $Y_{i-1}Y_i$? – we account the fact that only b_i gives information about its corresponding Y_i. Because a b_i symbol gives information only about its corresponding Y_i, in our analysis we consider independently the pairs (Y_i,b_i).

Taking into account the independency of all the pairs (Y_i,b_i), the conditional entropy $H(Y_{i-1}Y_i|b_{i-1}b_i)$ could be

expressed as the sum of $H(Y_{i-1}|b_{i-1})$ and $H(Y_i|b_i)$:

$$H(Y_{i-1}Y_i|b_{i-1}b_i) = H(Y_{i-1}|b_{i-1}) + H(Y_i|b_i) = 2. \quad (15)$$

From $H(Y_i) = 2$ we can deduce that $H(Y_{i-1}Y_i) = 4$. Therefore, the information about $Y_{i-1}Y_i$ gained by the eavesdropper is

$$I(Y_{i-1}Y_i; b_{i-1}b_i) = H(Y_{i-1}Y_i) - H(Y_{i-1}Y_i|b_{i-1}b_i) = 4 - 2 = 2 \text{ bits}. \quad (16)$$

That is, from the eavesdroppers point of view only four equiprobable four-bit strings $Y_{i-1}Y_i$ (out of 16) are possible to occur for a given $b_{i-1}b_i$. Each of these four equiprobable four-bit strings correspond to one of the four possible two-bit strings X_i (00,01,10,11), as can be seen in the encoding tables. This implies that $H(X_i|b_{i-1}b_i) = 2$. So, the information about X_i gained by the eavesdropper is

$$I(X_i; b_{i-1}b_i) = H(X_i) - H(X_i|b_{i-1}b_i) = 2 - 2 = 0 \text{ bits}. \quad (17)$$

In this way, we prove that the proposed protocol meets requirement (1).

Proof that the requirement (2) is met: If Eve gains information about the symbol X_0, the proposed scheme becomes more insecure. This is so because X_0 is the root, the foundation of the proposed encoding. Let us now analyse if Eve can gain any information about X_0. In this regard, we should prove that (a) knowing Y_0 does not give any information about X_0, i.e., $I(X_0; Y_0) = 0$, and that (b) knowing all the b_js does not give any information about $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1)$, i.e., $I(\text{XOR}; b_j) = 0$. We start off with proving (a).

It is known that the oddness of the number of 1s in a finite-size cryptographic key (random binary string) is a random variable with uniform distribution, i.e., $\text{XOR}(x_i) \in \{0, 1\} \sim$ unif, where $\text{XOR}(x_i)$ indicates performing XOR operation over all the bits x_i of a key string.

According to the encoding (see Sect. 2.1), Y_0 depends on $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1)$, and X_0. Because $H(Y_i) = 2$, as stated in the beginning of this section, we can assume that $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1) \in \{0, 1\} \sim$ unif. That is, the oddness of 1s in the MSBs (or LSBs) of a two-bit string Y is a random variable with uniform distribution – if we perform XOR operation on the all odd (or even) bits of a finite-size random sequence, the output of that operation is completely uncertain ($H(\text{XOR}) = 1$). Therefore, because Y_0 is a function of random variables ($Y_0 = f(\text{XOR}(Y_j^0), \text{XOR}(Y_j^1), X_0)$), then Y_0 itself is a random variable, i.e., $Y_0 \in \{0,1\}^2 \sim$ unif. Also, we know from the encoding (see Tab. 2) that each possible Y_0 can correspond to any possible X_0 (00,01,10, or 11). So, taking account of the later and that $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1) \in \{0,1\} \sim$ unif, X_0, $Y_0 \in \{0, 1\}^2 \sim$ unif, we then have [25]

$$H(X_0|Y_0) = \sum_{k=0}^{3} \Pr(Y_0 = y_k) H(X_0|Y_0 = y_k) = 2, \quad (18)$$

where $y_k \in \{y_0 = 00,\ y_1 = 01,\ y_2 = 10,\ y_3 = 11\}$.

Thus,

$$I(X_0; Y_0) = H(X_0) - H(X_0|Y_0) = 2 - 2 = 0 \text{ bits}. \quad (19)$$

We now begin proving (b). The values of $\text{XOR}(Y_j^0)$ and $\text{XOR}(Y_j^1)$ depend on the numbers (the oddness) of 00s, 01s, 10s, 11s in the string Y (excluding Y_0). In the finite-size random strings one is preliminary unaware of the exact numbers of the two-bit symbols, i.e., one is unaware of the values of $\text{XOR}(Y_j^0)$ and $\text{XOR}(Y_j^1)$. Also, despite knowing the b_j, the eavesdropper is uncertain about the values of Y_j^0 and Y_j^1 ($H(Y_j|b_j) = 1$). Because of the above-stated facts, we are right to assume that even knowing the $b_j s$ the eavesdropper is uncertain about the values of $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1)$, i.e., $H(\text{XOR}^0|b_j) = H(\text{XOR}^1|b_j) = 1$. Therefore, the information about $\text{XOR}(Y_j^0)$, $\text{XOR}(Y_j^1)$ gained by the eavesdropper is

$$I(\text{XOR}^r; b_j) = H(\text{XOR}^r) - H(\text{XOR}^r|b_j) = 1 - 1 = 0 \text{ bits}, \quad (20)$$

where $r \in \{0,1\}$. In this way, we prove that the proposed protocol meets requirement (2).

We should mention that the proposed communication scheme has a drawback, but it is not a significant drawback: Knowing b_i and Y_i give 1 bit of information about the next message symbol X_{i+1}. This drawback can be overcome by using an encoding in which the values of $Y_i s$ depend on their corresponding $X_{i-1} s$, but not on $Y_{i-1} s$. This approach of encoding, however, makes the decoding more cumbersome.

6 Summary

In summary, the paper presents a novel quantum channel compression (QCC) process, which reduces the quantum resources used in a quantum secure communication (QSC) protocol. This process uses encoding, messaging during eavesdropping check procedure, and decoding. On the basis of QCC, a novel teleportation-based direct secure quantum communication protocol (T-DSQC) is established for cryptographic key exchange (distribution). This protocol can be regarded as an enhancement of the common teleportation-based protocol [9]. The enhancement lies in transferring two bits per teleportation procedure, unlike the work in [9], where one bit is transferred per teleportation procedure.

The newly established protocol is characterized with efficiency greater than those of the protocols presented in [9–11], as shown in Table 3. It obtains efficiency of 0.286 (28.6%).

In this article, we also present a detailed security analysis to the proposed protocol, as can be seen in Section 5.2. It is proved that the protocol is completely secure against attacks launched both on the quantum and classical channels used in the scheme – because the proposed protocol is based on that presented in [9], we assume that it is secure against quantum attacks as well.

The work is supported by the project ДН07/10-2016 and programme YRPD, funded by National Science Fund, Ministry of Education and Science, Bulgaria.

Author contribution statement

G.B. developed the theoretical formalism and performed the calculations. Both authors contributed to the final version of the manuscript. R.D. supervised the project.

References

1. C. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 10–12 December 1984* (1984), p. 175
2. A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
3. C. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)
4. G. Long, X. Liu, Phys. Rev. A **65**, 032302 (2002)
5. F. Deng, G. Long, Phys. Rev. A **69**, 052319 (2004)
6. F. Deng et al., Phys. Rev. A **68**, 042317 (2003)
7. C. Tsai et al., Eur. Phys. J. D **61**, 783 (2011)
8. C. Wang et al., Phys. Rev. A **71**, 044305 (2005)
9. F. Yan, X. Zhang, Eur. Phys. J. B **41**, 75 (2004)
10. D. Joy et al., Quantum Inf. Process. **16**, 157 (2017)
11. X. Xiu et al., Commun. Theor. Phys. **51**, 429 (2009)
12. H. Cao, H. Song, Phys. Scr. **74**, 572 (2006)
13. L. Dong et al., Commun. Theor. Phys. **49**, 1495 (2008)
14. N. Qin et al., Int. J. Theor. Phys. **52**, 22 (2013)
15. S. Hassanpour, M. Houshmand, Quantum Inf. Process. **14**, 739 (2015)
16. X. Li et al., J. Korean Phys. Soc. **49**, 1354 (2006)
17. Z. Cao et al., Int. J. Theor. Phys. **57**, 3632 (2018)
18. T. Gao et al., Chin. Phys. **14**, 893 (2005)
19. A. Banerjee, A. Pathak, Phys. Lett. A **376**, 2944 (2012)
20. G. Bebrov, R. Dimova, Int. J. Theor. Phys., in press, DOI:10.1007/s10773-019-04336-9
21. Ch. Bennet, G. Brassard, C. Crepeau, U. Maurer, IEEE Trans. Inf. Theor. **41**, 1915 (1995)
22. G. Brassard, L. Salvail, in *Advances in Cryptology – EUROCRYPT '93. EUROCRYPT 1993, Lecture Notes in Computer Science* (Springer, Berlin, Heidelberg, 1994), Vol. 765, pp. 386–397
23. A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000)
24. C. Shannon, Bell Syst. Tech. J. **27**, 379 (1948)
25. M. Wilde, in *Quantum Information Theory* (Cambridge University Press, UK, 2017), p. 275